

①9 RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

①1 N° de publication :
(à n'utiliser que pour les
commandes de reproduction)

2 703 859

②1 N° d'enregistrement national :

93 04262

⑤1 Int Cl⁵ : H 03 M 13/22 , H 04 L 12/00 , G 06 F 11/08

①2

DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 09.04.93.

③0 Priorité :

④3 Date de la mise à disposition du public de la
demande : 14.10.94 Bulletin 94/41.

⑤6 Liste des documents cités dans le rapport de
recherche préliminaire : *Se reporter à la fin du
présent fascicule.*

⑥0 Références à d'autres documents nationaux
apparentés :

⑦1 Demandeur(s) : *Société dite : THOMSON-CSF
(Société anonyme) — FR.*

⑦2 Inventeur(s) : Guilbaud Bertrand et Henry Pierre.

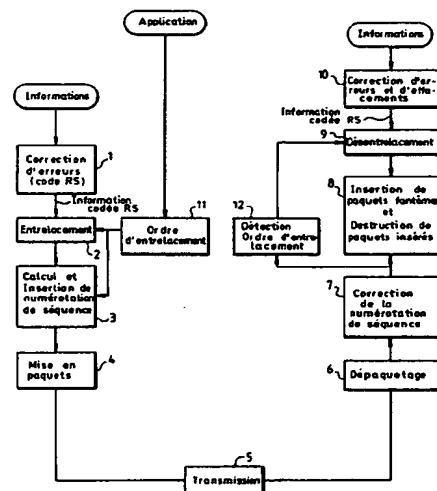
⑦3 Titulaire(s) :

⑦4 Mandataire : Lingot Georges.

⑤4 Procédé de gestion dynamique de la capacité de correction d'une couche d'adaptation à l'ATM.

⑤7 Le procédé consiste à entrelacer des informations codées Reed-Solomon sur une profondeur variable dépendante de l'application avant leur transmission en paquets sur un réseau ATM et à effectuer à la réception un désentrelacement se synchronisant dynamiquement et automatiquement quelque soit la profondeur d'entrelacement et ce avant le décodage Reed-Solomon qui corrige les erreurs et les effacements générés par la transmission.

Applications: Télévision Haute Définition et compatibles, Son Haute Fidélité et compatibles, Visiotéléphonie, Multiplex de tous ces signaux (par exemple MPEG 1 et 2).



FR 2 703 859 - A1



Procédé de gestion dynamique de la capacité de correction d'une couche d'adaptation à l'ATM

5 La présente invention concerne un procédé de gestion dynamique de la capacité de correction d'une couche d'adaptation à l'ATM dite AAL pour services audiovisuels interactifs et distributifs, ATM étant l'abréviation de "Asynchronous Transfer Mode" et AAL l'abréviation de "ATM Adaptation Layer" dans le langage anglo-saxon. La technologie ATM consiste en la
10 transmission des données utiles sous la forme de cellules constituées de cinq octets d'en-tête et de quarante huit octets d'informations.

Les recommandations CCITT I.321, I.361, I.362 et I.363 définissent les différentes couches du modèle de référence, leurs fonctions et leurs domaines d'application.

15 La recommandation I.362 du CCITT définit quatre classes de services caractérisés par leurs débits, leurs modes de connexion et les niveaux de relation temporelle entre émetteurs et récepteurs.

La recommandation I.363 du CCITT définit quatre types d'adaptation à l'ATM utilisables dans chaque classe de service.

20 Les transmissions audiovisuelles sont caractérisées par des débits d'information très différents, pouvant varier de 64 Kbit/s pour la visiophonie de basse qualité, à 256 à 512 Kbit/s pour le son HiFi, à 2 Mbit/s pour la visioconférence, jusqu'à 8 Mbit/s et 34 Mbit/s pour la distribution de télévision standard et de télévision haute définition. Les contraintes temps réel
25 inhérentes à la transmission de ce type de signaux interdisent la réémission des informations lorsque, dans le train binaire reçu, des erreurs sont détectées.

Dans la recommandation I.363 du CCITT, une méthode optionnelle de correction des erreurs bits et des pertes de cellules est proposée pour
30 l'AAL de type 1. Basée sur l'utilisation d'un code Reed-Solomon (128,124) sur le corps de Galois GF(256) encore noté GF(2^8) et d'un entrelaceur d'ordre 47 cette méthode n'est applicable qu'aux services vidéo distribués.

Une des particularités de cette technique est que le temps de traitement des informations est d'autant plus long que le débit du service traité est

faible. Ce temps d'entrelacement est approximativement égal au temps de remplissage de la mémoire d'entrelacement :

$$T_{\text{codeur}} = 128 \times 47 \times 8 / \text{débit}$$

$$T_{\text{décodeur}} = 128 \times 47 \times 8 / \text{débit}$$

5 Cette caractéristique s'avère être un inconvénient majeur dans le cas particulier d'applications bas débits et/ou interactives telles que le son haute fidélité ou la visiophonie par exemple, pour lesquelles le temps de traitement de bout en bout doit être aussi court que possible pour que la qualité de service soit bonne.

10 Les propositions faites à ce jour à ce niveau du système de télécommunications, pour remédier à ce problème, se bornent à réduire la taille de la matrice d'entrelacement en utilisant un code Reed-Solomon différent de celui déjà recommandé (par exemple RS (32,30) sur GF(256) couplé à un entrelaceur d'ordre 47 : à débit identique, le temps de traitement est ici
15 divisé par quatre).

Ces propositions présentent les divers inconvénients majeurs suivants :

- incompatibilité entre des codes Reed-Solomon différents :

- RS (128,124)*47 et RS(32,30)*47 par exemple.

20 - codes RS sur GF(256) réduits donc pas utilisés au maximum de leur rendement.

- réalisation matérielle de composants VLSI et même de cartes électroniques offrant les fonctionnalités de l'AAL de type 1 pour différents types de services (vidéo, audio, visiophonie ...) très complexe puisque seule la
25 hauteur de la matrice d'entrelacement est constante alors que sa longueur et surtout son code RS sur GF(256) sont modifiés.

L'invention a pour but de pallier à ces défauts, en proposant l'utilisation d'un seul et même code Reed-Solomon sur GF(256), quel que soit le type d'application envisagée, couplé à une mémoire d'entrelacement de
30 taille variable choisie au codeur et à un synchroniseur d'entrelacement automatique au décodeur.

A cet effet, l'invention a pour objet un procédé d'entrelacement de données issues de services audiovisuels distributifs et interactifs et codées Reed-Solomon pour les protéger contre les erreurs bits et les pertes de cel-
35 lules dans un réseau temporel asynchrone caractérisé en ce qu'il consiste à

conserver le même code Reed-Solomon quelque soit l'application envisagée, à entrelacer ces données codées RS sur une profondeur variable fixée par l'application avant leur transmission en paquets ou cellules sur le réseau, à effectuer un désentrelacement des informations contenues dans
5 les paquets ou cellules, sans pour autant avoir recours à des indications "SAR-PDU" autres que celles décrites dans la recommandation I.363 du CCITT pour synchroniser le mécanisme et à corriger au moyen du code Reed-Solomon les erreurs et les effacements dans les symboles restitués.

D'autres caractéristiques et avantages de l'invention apparaîtront ci-après à la lumière de la description qui suit faite en regard des dessins annexés qui représentent :

- La figure 1 les différentes étapes du procédé selon l'invention mises sous la forme d'un organigramme,
- La figure 2 un synoptique du mécanisme d'entrelacement permettant
15 la mise en oeuvre du procédé à l'émetteur selon la figure 1.
- La figure 3 un synoptique du mécanisme d'entrelacement permettant la mise en oeuvre du procédé au récepteur selon la figure 1.
- La figure 4 un format de segmentation de cellules ATM, pour une adaptation de type 1 selon la recommandation I.363 du CCITT.
- 20 - La figure 5 un schéma d'organisation d'un dispositif d'entrelacement permettant la mise en oeuvre du procédé selon la figure 1 pour un premier exemple d'application.
- La figure 6 un schéma d'organisation d'un dispositif d'entrelacement différent permettant la mise en oeuvre du procédé selon la figure 1 pour un
25 autre exemple d'application.
- La figure 7 un schéma d'organisation d'un dispositif d'entrelacement différent permettant la mise en oeuvre du procédé selon la figure 1 pour un troisième type d'application.
- La figure 8 un schéma détaillé du format de segmentation des
30 cellules ATM permettant la mise en oeuvre des différents dispositifs d'entrelacement dans un même et unique produit.
- Les figures 9, 10, 11, 12, 13, les performances, en terme de taux d'erreurs résiduelles après correction pour des taux d'erreurs bits et pertes de cellules donnés, des diverses associations données à titre d'exemples
35 réalistes et ce pour différents débits.

Le procédé de protection contre les erreurs bits et pertes de cellules ATM selon l'invention est illustré par les étapes 1 à 12 de la figure 1. Il consiste à l'étape 1 à convertir chaque symbole ou octet représentatif du signal source (audio, vidéo, visiophonie, multiplex de type MPEG 1 ou 2...) en mot
 5 de code de Reed-Solomon de la façon décrite par exemple page 207 du livre de G. Cullmann ayant pour titre "Codes détecteurs et correcteurs d'erreurs" publié par DUNOD 1967 dans la collection "Initiation aux nouveautés de la science" ou encore de la façon décrite pages 304-308 du livre de Bernard Sklar intitulé "DIGITAL COMMUNICATIONS Fundamentals and
 10 Applications" publié par Prentice Hall 1988. Les informations codées obtenues forment des mots des codes notés $C(N, K, D)$ ou $RS(N, K, D)$ de distance de Hamming D , de longueur N en nombre de symboles et renfermant K informations utiles.

Ces informations sont entrelacées à l'étape 2 au moyen d'un dispositif
 15 d'entrelacement agencé suivant le schéma de principe de la figure 2, encore décrit, sous forme d'exemples dans les figures 5, 6 et 7. Suivant ce dispositif, les mots de N symboles sont mémorisés horizontalement dans la mémoire d'entrelacement d'une capacité égale à :

$$C_1 = N * L$$

20 où L est la profondeur d'entrelacement, encore appelé ordre d'entrelacement, et est fonction de l'application envisagée ou encore de la capacité de correction nécessaire pour offrir une bonne qualité de service. Les champs d'information "SAR-PDU payload" des cellules ATM sont obtenus en lisant verticalement la mémoire d'entrelacement comme décrit sur les exemples
 25 des figures 5, 6 et 7 où les numéros mis en exposant indiquent le numéro de la cellule d'appartenance dans la matrice :

3^2 représente l'octet n°3 de la cellule n°2.

Le calcul de numéros de séquences qui est effectué à l'étape 3 et leur insertion conduit à une segmentation des cellules (SAR-PDU) suivant un
 30 format représenté à la figure 4 et détaillé à la figure 8 conforme à la recommandation CCITT I.363. La cellule ATM comporte donc 40 bits d'en-tête "Header" et 384 bits de "SAR-PDU" dont :

- 4 bits SN de numéro de séquence et 4 bits SNP de protection du champ SN contre les erreurs formant le "SAR-PDU header"
- 35 - 376 bits d'informations formant le "SAR-PDU payload".

Le tout forme une cellule de $5+48 = 53$ octets. Le champ SN est lui-même divisé en deux parties (figure 8), l'une, constituée des 3 bits les moins significatifs permettant une numérotation modulo 8, l'autre, constituée du bit le plus significatif, aussi appelé CSI, permettant l'insertion d'une indication de début de matrice d'entrelacement par exemple.

En réception le dépaquetage des cellules est effectué à l'étape 6. Les cellules sont restituées dans le format SAR-PDU de la figure 4 et une correction des numéros de séquences a lieu à l'étape 7 suivi à l'étape 8, par le remplacement des cellules perdues détectées grâce à la vérification de l'intégrité de la numérotation de séquence, par des cellules "fantômes" dans le dispositif de désentrelacement ainsi que par la destruction des cellules insérées détectées.

Un désentrelacement des données a alors lieu à l'étape 9 au moyen d'un dispositif de désentrelacement symétrique du dispositif de l'étape 2 utilisant une mémoire de capacité :

$$C_2 = L * N$$

Naturellement l'opération de désentrelacement de l'étape 9 doit être synchronisée avec les indications de début de matrice de désentrelacement ainsi qu'avec l'insertion des paquets fantômes et/ou la destruction des paquets insérés de l'étape 8 pour que le mécanisme qui consiste en l'écriture verticale des champs "SAR-PDU payload" des cellules reçues suivi de la lecture horizontale des mots de code Reed-Solomon reconstitués soit efficace.

Ces codes sont ensuite analysés à l'étape 10 pour effectuer les corrections d'erreurs et d'effacements.

Le procédé de l'invention qui vient d'être décrit s'applique à des configurations de matrices d'entrelacement et de codes Reed-Solomon très différentes à condition que le nombre d'octets contenus dans la matrice soit un multiple de 47 de façon à avoir un nombre entier de champs "SAR-PDU payload" dans une matrice, quelle que soit la profondeur de celle-ci, ceci pour simplifier la gestion du système. Il est important de noter que ce procédé peut tout aussi bien s'appliquer à des méthodes d'entrelacement différentes, par exemple basées sur des écritures horizontales des mots de code RS et des lectures diagonales des tableaux ainsi réalisés.

Les exemples qui suivent sont basés sur des matrices à structure rectangulaire (balayage horizontal et vertical) dans un souci de simplification de la démonstration :

- code RS(47,44) couplé à des matrices de profondeur 24 et 12
- 5 - code RS(188,172) couplé à des matrices de profondeur 24, 12, 6 et 3.

Cependant pour un maximum d'efficacité il est préférable de fixer un code Reed-Solomon aussi peu réduit que possible pour toutes les applications et de "jouer" uniquement sur la taille de la matrice d'entrelacement pour s'adapter aux diverses applications supportées par l'AAL de type 1. Pour ce faire on prendra la précaution de choisir une longueur de mot de code Reed-Solomon sur GF(256) multiple de 47 (en octets) aussi proche que possible de 255 (2^8-1). La longueur N du mot de code Reed-Solomon qui peut donc prendre, pour un code sur GF(256) les valeurs suivantes : N1 = 47, N2 = 94, N3 = 141, N4 = 188, N5 = 235 est choisie égale à N5 qui offrira le meilleur rendement. On note que $235 = 5 \times 47$.

Des exemples sont présentés sur les figures 5, 6 et 7 qui permettent de comprendre l'originalité du dispositif d'entrelacement. Dans le cas des réseaux ATM, la longueur R du champ "SAR-PDU payload" de la cellule ATM est égale à 47 octets. N longueur du mot du code RS et L profondeur de la matrice d'entrelacement peuvent donc être choisis respectivement égaux à 235 et 24 (figure 5), ou 235 et 12 (figure 6), ou 235 et 6 (figure 7) (tout autre valeur de L est acceptable, par exemple L = 5 ...). K, le nombre d'octets utiles dans le mot de code Reed-Solomon et par conséquent D, distance de Hamming du code de Reed-Solomon ne modifient en rien le principe d'entrelacement. Le choix de D sera fonction de plusieurs paramètres tels la redondance acceptée pour protéger le service, les caractéristiques du système de transmission et les performances attendues du mécanisme de protection.

Dans un souci de simplification de la description du procédé, un exemple réaliste est maintenant décrit. Les paramètres choisis peuvent évidemment être modifiés.

Le taux de redondance généralement considéré comme acceptable pour effectuer de la correction d'erreurs dans le domaine des télécommuni-

cations numériques se situe entre 5% et 10%. Ceci est d'autant mieux accepté que les procédés de compression de l'information actuellement développés permettent d'envisager des débits utiles compris entre 30 Mbit/s et 40 Mbit/s pour des signaux de télévision haute définition comprimés, débits qui ne sont pas aussi critiques pour un réseau large bande asynchrone que pouvaient l'être les 140 Mbit/s annoncés ces dernières années.

Le code Reed-Solomon choisi pour cet exemple est donc un RS(235,219,17), qui ajoute une redondance de 7,3% aux informations utiles. Il peut être entrelacé sur des profondeurs différentes dépendantes des applications comme illustré dans le tableau ci-dessous où les valeurs de R sont données à titre d'exemples :

| Profondeur | Nbre de cellules | Gamme de débits | Nbre de cellules corrigeables | Retard max |
|------------|------------------|-------------------|----------------------------------|------------|
| R = 24 | n = 120 | 10 Mb/s_140 Mb/s | 8/120 | 4,5 ms |
| R = 12 | n = 60 | 4 Mb/s_10 Mb/s | 4/60 | 5,7 ms |
| R = 6 | n = 30 | 0,5 Mb/s_4 Mb/s | 2/30 | 22,8 ms |
| R = 3 | n = 15 | 128 Kb/s_0,5 Mb/s | 1/15 | 44,1 ms |

Si pour les débits les plus élevés le retard de traitement reste négligeable (<10 ms), celui-ci devient important à 128 Kbit/s mais cependant encore nettement inférieur aux temps de traitement des algorithmes de compression utilisés (entre 150 ms et 300 ms).

Les figures 9, 10, 11, 12 et 13 montrent les performances des divers exemples donnés ci-dessus pour des débits binaires respectivement de 40, 10, 4, 0,5 Mbit/s et 128 Kb/s. Les graphes correspondants comportent en ordonnée le taux d'erreur résiduel en fonction du taux d'erreur entrant, pour des entrelacements de codes RS(235, 219) sur respectivement 24 lignes (courbe A), 12 lignes (courbe B), 6 lignes (courbe C) et 3 lignes (courbe D). On y voit clairement que si la réduction de la taille de la matrice d'entrelacement diminue les performances du système de correction pour un débit de service donné, cela n'est pas le cas quand on passe d'une catégorie de débits à une autre. Le défaut de cette technique de correction est qu'elle se comporte moyennement devant des pertes consécutives de cellules mais cet événement reste extrêmement rare pour des services à

faible débit. Si malheureusement, sur une transmission particulière, cela se produisait trop souvent il suffirait alors de passer à la matrice de taille supérieure pour augmenter la capacité de correction. Ceci augmenterait du même coup le temps de traitement.

REVENDEICATIONS

1. Procédé d'entrelacement de données issues de services audiovisuels distributifs et interactifs et codées Reed-Solomon pour les protéger
5 contre les erreurs bits et les pertes de cellules spécifiques des réseaux temporels asynchrones caractérisé en ce qu'il consiste à conserver le même code Reed-Solomon quelle que soit l'application envisagée, à entrelacer (2) ces données codées RS sur une profondeur variable fixée par l'application avant leur transmission en paquets ou cellules sur le réseau, à effectuer un
10 désentrelacement (9) des informations contenues dans les paquets ou cellules, à l'aide de paramètres décrits dans la recommandation I.363 du CCITT (CSI bit) pour synchroniser dynamiquement le mécanisme et à corriger (10) au moyen du code Reed-Solomon les erreurs et les effacements dans les symboles restitués.
- 15 2. Procédé selon la revendication 1 caractérisé en ce que l'entrelacement (2) consiste à mémoriser ligne par ligne les informations codées en mots de Reed-Solomon de N symboles dans une mémoire et à lire cette mémoire colonne par colonne ou diagonale par diagonale pour former les champs "SAR-PDU payload" des cellules ATM ceci en prenant la précaution
20 de choisir N multiple de la taille de ces champs "SAR-PDU payload".
3. Procédé selon l'une quelconque des revendications 1 et 2 caractérisé en ce que le désentrelacement (9) consiste à mémoriser les champs "SAR-PDU payload" colonne par colonne ou diagonale par diagonale dans une mémoire et à lire cette mémoire ligne par ligne pour
25 reformer les mots de code Reed-Solomon.
4. Procédé selon l'une quelconque des revendications précédentes caractérisé en ce que la taille des mémoires d'entrelacement et de désentrelacement est variable pour un mot de code Reed-Solomon donné et dépend de l'application et/ou des conditions de transmissions et/ou du coût du sys-
30 tème développé.
5. Procédé selon l'une quelconque des revendications précédentes caractérisé en ce que les codes Reed-Solomon sont des codes RS(N, K, D) sur $GF(2^n)$ de longueur de code N multiple de la taille d'un champ "SAR-PDU payload" et de préférence pour une efficacité maximum le plus proche
35 possible de 2^n mais en y restant inférieur.

6. Procédé selon l'une quelconque des revendications précédentes caractérisé en ce qu'il consiste à utiliser la capacité de correction des effacements (erreurs probables déjà localisées).

5 7. Procédé selon l'une quelconque des revendications précédentes caractérisé en ce que chaque symbole a la dimension d'un mot de n bits si le code correcteur d'erreurs est défini sur $GF(2^n)$. Dans le cas de l'ATM, $n = 8$.

10 8. Procédé selon l'une quelconque des revendications précédentes caractérisé en ce qu'il consiste à insérer des cellules fantômes dans un tableau de désentrelacement en marquant chaque symbole pour qu'il soit interprété comme un effacement par le décodeur Reed-Solomon et ce en synchronisme avec la variation dynamique de la taille de la profondeur d'entrelacement.

1111

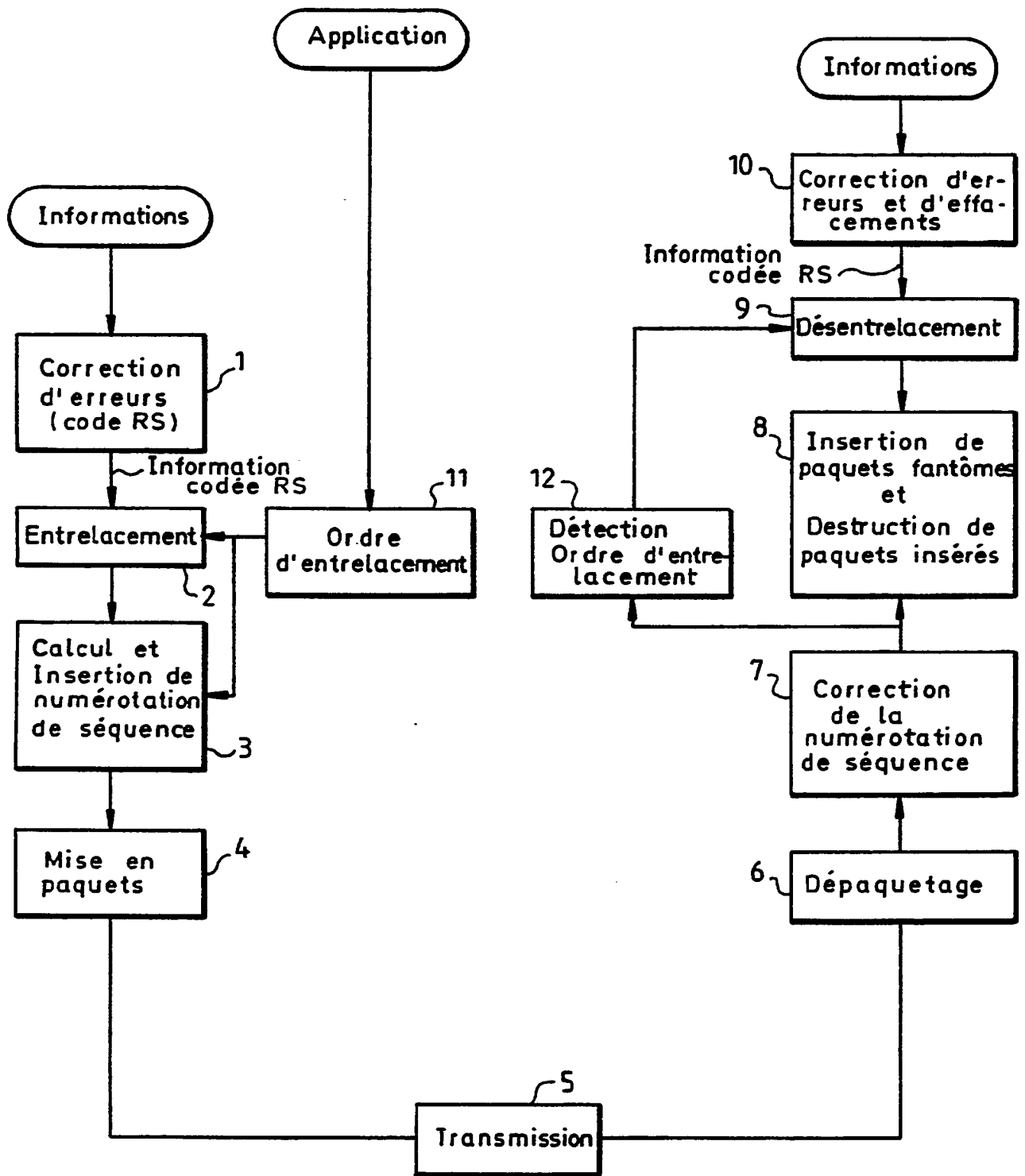


FIG.1

2/11

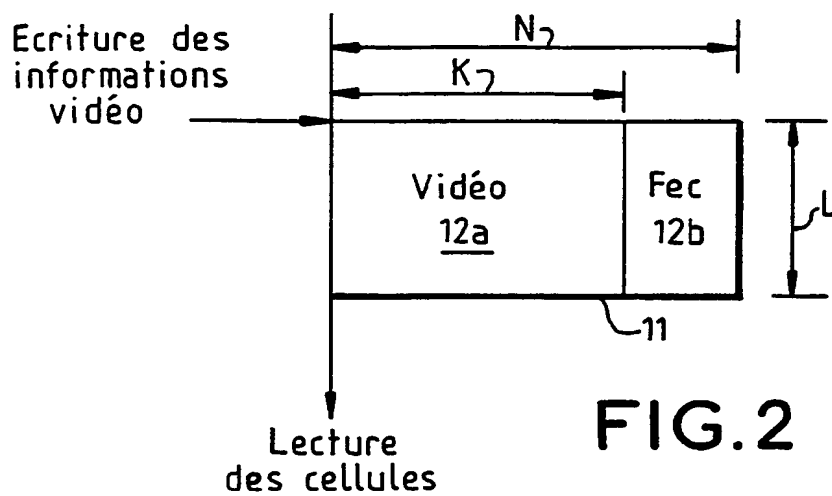


FIG. 2

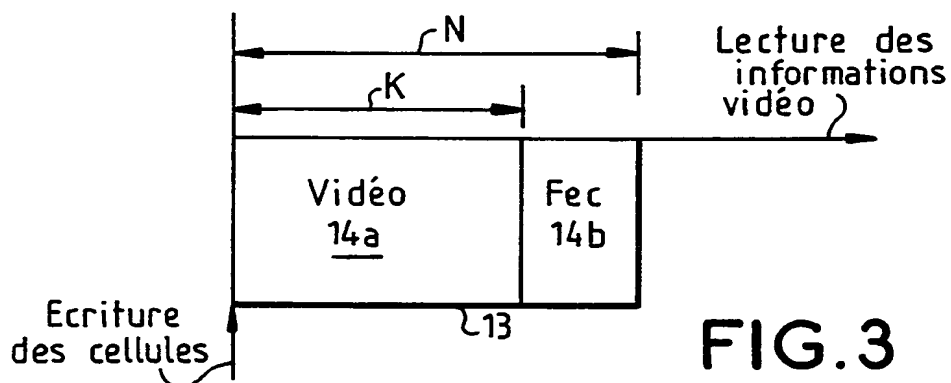


FIG. 3

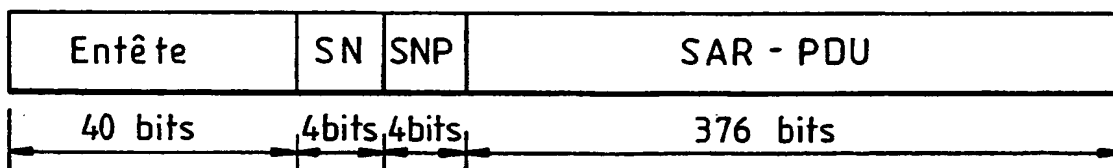
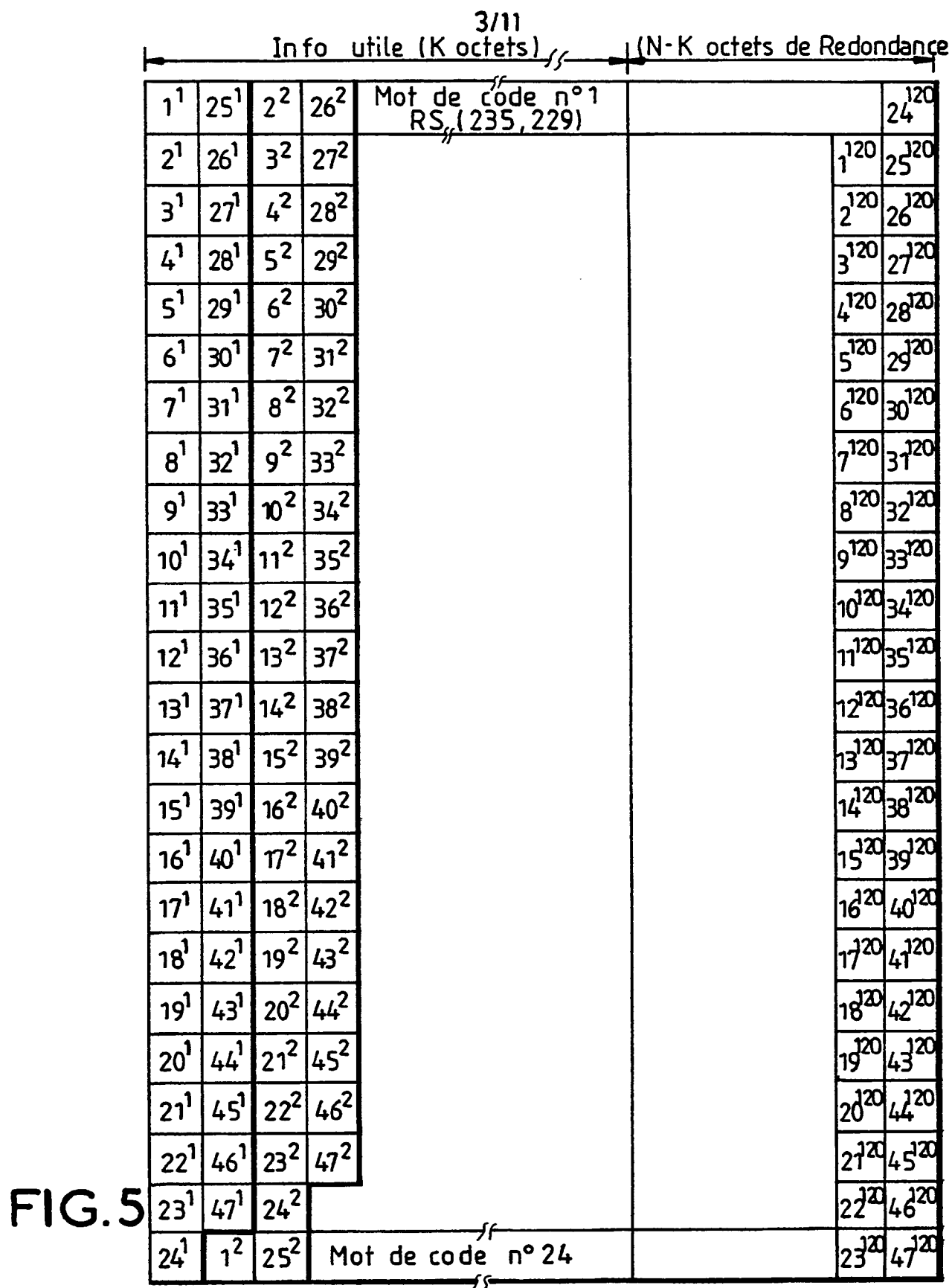


FIG. 4



| | | | | | | | | | | | | | | | | | |
|--------------------------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|------------------|--|--|--|-----------------|------------------|------------------|------------------|------------------|------------------|
| Mot de code n°1 RS (N.K.D.) | | | | | | | | | | | | 1 ⁶⁰ | 12 ⁶⁰ | 24 ⁶⁰ | 36 ⁶⁰ | | |
| 1 ¹ | 13 ¹ | 25 ¹ | 37 ¹ | 2 ² | 14 ² | 26 ² | 38 ² | | | | | | | 2 ⁶⁰ | 13 ⁶⁰ | 25 ⁶⁰ | 37 ⁶⁰ |
| 2 ¹ | 14 ¹ | 26 ¹ | 38 ¹ | 3 ² | 15 ² | 27 ² | 39 ² | | | | | | | 3 ⁶⁰ | 14 ⁶⁰ | 26 ⁶⁰ | 38 ⁶⁰ |
| 3 ¹ | 15 ¹ | 27 ¹ | 39 ¹ | 4 ² | 16 ² | 28 ² | 40 ² | | | | | | | 4 ⁶⁰ | 15 ⁶⁰ | 27 ⁶⁰ | 39 ⁶⁰ |
| 4 ¹ | 16 ¹ | 28 ¹ | 40 ¹ | 5 ² | 17 ² | 29 ² | 41 ² | | | | | | | 5 ⁶⁰ | 16 ⁶⁰ | 28 ⁶⁰ | 40 ⁶⁰ |
| 5 ¹ | 17 ¹ | 29 ¹ | 41 ¹ | 6 ² | 18 ² | 30 ² | 42 ² | | | | | | | 6 ⁶⁰ | 17 ⁶⁰ | 29 ⁶⁰ | 41 ⁶⁰ |
| 6 ¹ | 18 ¹ | 30 ¹ | 42 ¹ | 7 ² | 19 ² | 31 ² | 43 ² | | | | | | | 7 ⁶⁰ | 18 ⁶⁰ | 30 ⁶⁰ | 42 ⁶⁰ |
| 7 ¹ | 19 ¹ | 31 ¹ | 43 ¹ | 8 ² | 20 ² | 32 ² | 44 ² | | | | | | | 8 ⁶⁰ | 19 ⁶⁰ | 31 ⁶⁰ | 43 ⁶⁰ |
| 8 ¹ | 20 ¹ | 32 ¹ | 44 ¹ | 9 ² | 21 ² | 33 ² | 45 ² | | | | | | | 9 ⁶⁰ | 20 ⁶⁰ | 32 ⁶⁰ | 44 ⁶⁰ |
| 9 ¹ | 21 ¹ | 33 ¹ | 45 ¹ | 10 ² | 22 ² | 34 ² | 46 ² | | | | | | | 10 ⁶⁰ | 21 ⁶⁰ | 33 ⁶⁰ | 45 ⁶⁰ |
| 10 ¹ | 22 ¹ | 34 ¹ | 46 ¹ | 11 ² | 23 ² | 35 ² | 47 ² | | | | | | | 11 ⁶⁰ | 22 ⁶⁰ | 34 ⁶⁰ | 46 ⁶⁰ |
| 11 ¹ | 23 ¹ | 35 ¹ | 47 ¹ | 12 ² | 24 ² | 36 ² | | Mot de code n°12 | | | | | | 12 ⁶⁰ | 23 ⁶⁰ | 35 ⁶⁰ | 47 ⁶⁰ |
| 12 ¹ | 24 ¹ | 36 ¹ | 1 ² | 13 ² | 25 ² | 37 ² | | | | | | | | | | | |

FIG. 6

| | | | | | | | | | | | | | | | | | | | | | | | | |
|----------------|----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|--------------------------------|-----------------|-----------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|
| 1 ¹ | 5 ¹ | 9 ¹ | 13 ¹ | 17 ¹ | 21 ¹ | 25 ¹ | 29 ¹ | 33 ¹ | 37 ¹ | 41 ¹ | 45 ¹ | Mot de code n°1 RS (N°,K,D) | 4 ²⁰ | 8 ²⁰ | 12 ²⁰ | 16 ²⁰ | 20 ²⁰ | 24 ²⁰ | 28 ²⁰ | 32 ²⁰ | 36 ²⁰ | 40 ²⁰ | 44 ²⁰ | |
| 2 ¹ | 6 ¹ | 10 ¹ | 14 ¹ | 18 ¹ | 22 ¹ | 26 ¹ | 30 ¹ | 34 ¹ | 38 ¹ | 42 ¹ | 46 ¹ | | 1 ²⁰ | 5 ²⁰ | 9 ²⁰ | 13 ²⁰ | 17 ²⁰ | 21 ²⁰ | 25 ²⁰ | 29 ²⁰ | 33 ²⁰ | 37 ²⁰ | 41 ²⁰ | 45 ²⁰ |
| 3 ¹ | 7 ¹ | 11 ¹ | 15 ¹ | 19 ¹ | 23 ¹ | 27 ¹ | 31 ¹ | 35 ¹ | 39 ¹ | 43 ¹ | 47 ¹ | | 2 ²⁰ | 6 ²⁰ | 10 ²⁰ | 14 ²⁰ | 18 ²⁰ | 22 ²⁰ | 26 ²⁰ | 30 ²⁰ | 34 ²⁰ | 38 ²⁰ | 42 ²⁰ | 46 ²⁰ |
| 4 ¹ | 8 ¹ | 12 ¹ | 16 ¹ | 20 ¹ | 24 ¹ | 28 ¹ | 32 ¹ | 36 ¹ | 40 ¹ | 44 ¹ | | Mot de code n°4 | 3 ²⁰ | 7 ²⁰ | 11 ²⁰ | 15 ²⁰ | 19 ²⁰ | 23 ²⁰ | 27 ²⁰ | 31 ²⁰ | 35 ²⁰ | 39 ²⁰ | 43 ²⁰ | 47 ²⁰ |

FIG.7

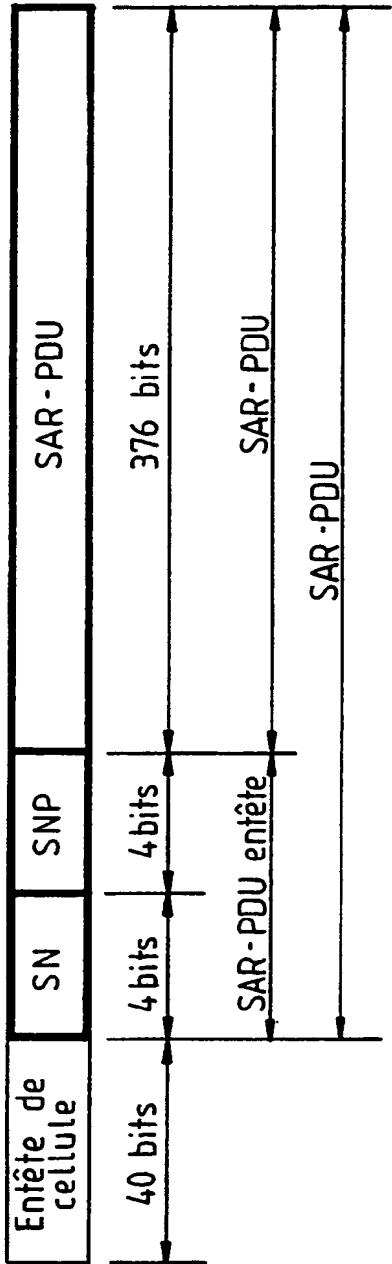


FIG. 8a

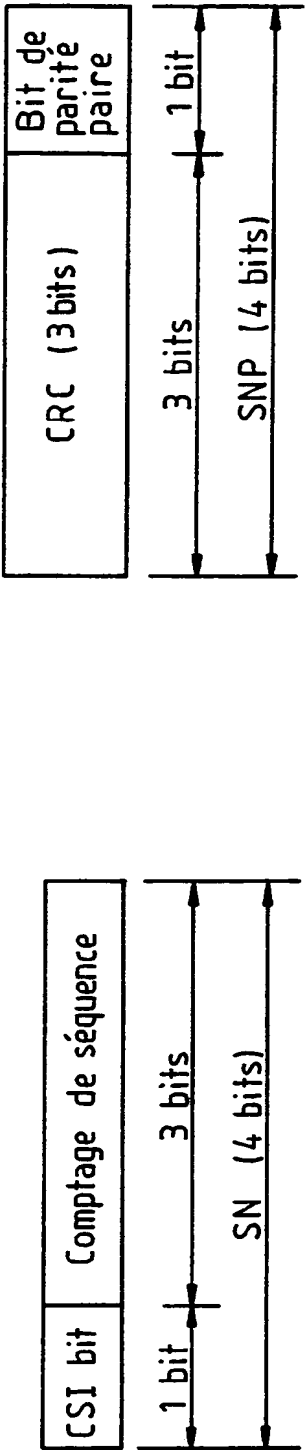


FIG. 8b

FIG. 8c

7/11

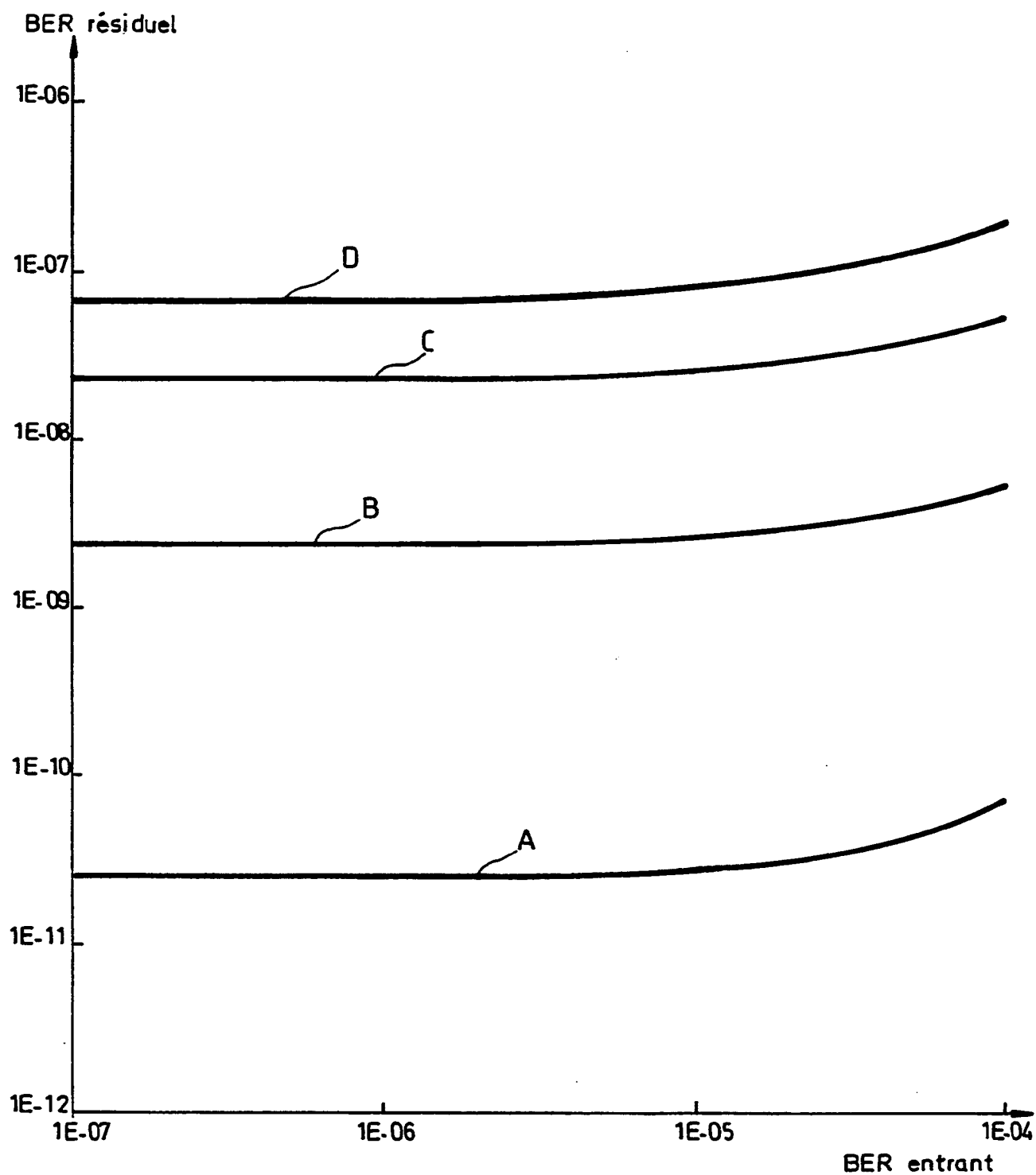


FIG.9

8/11

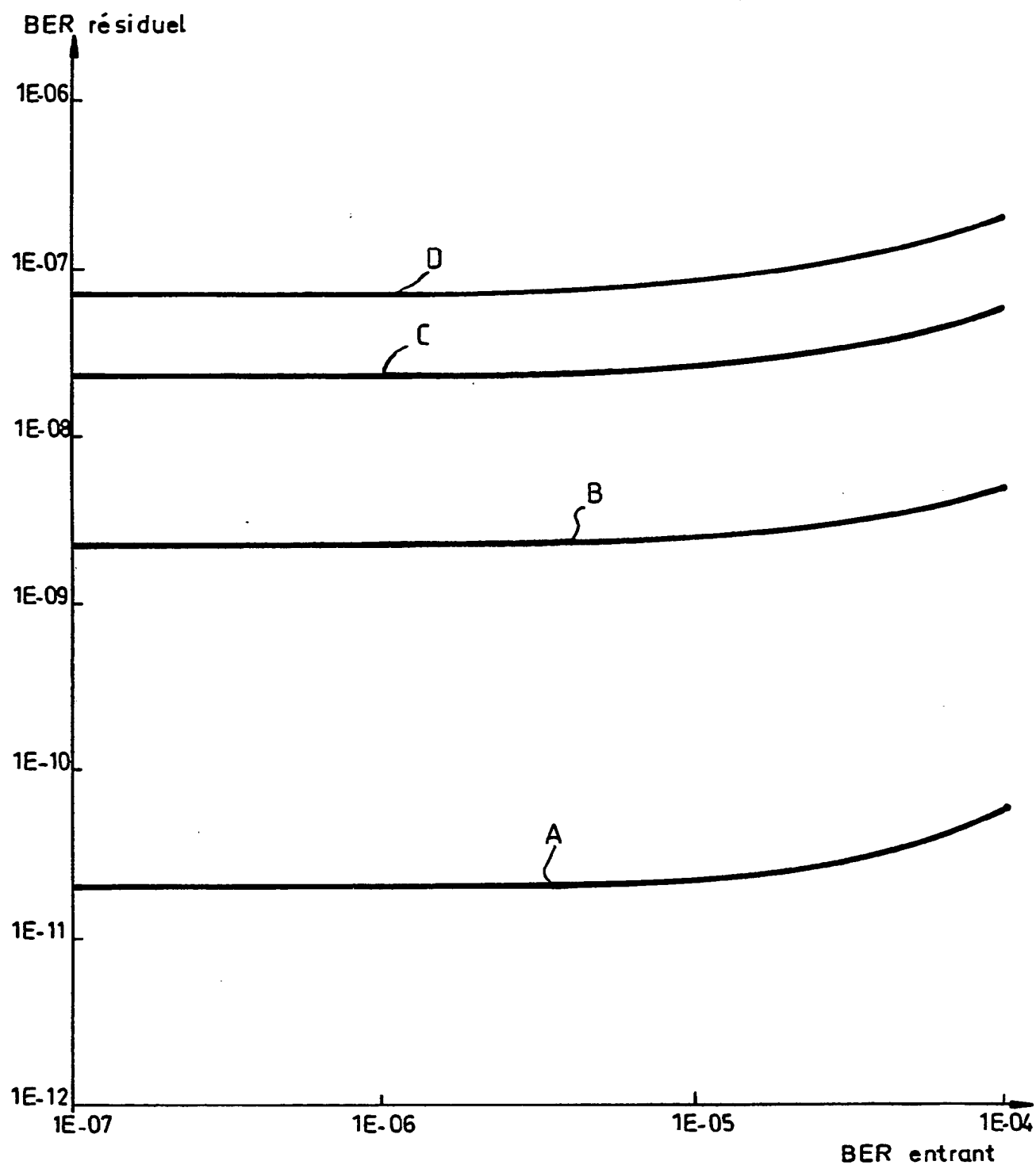


FIG.10

9/11

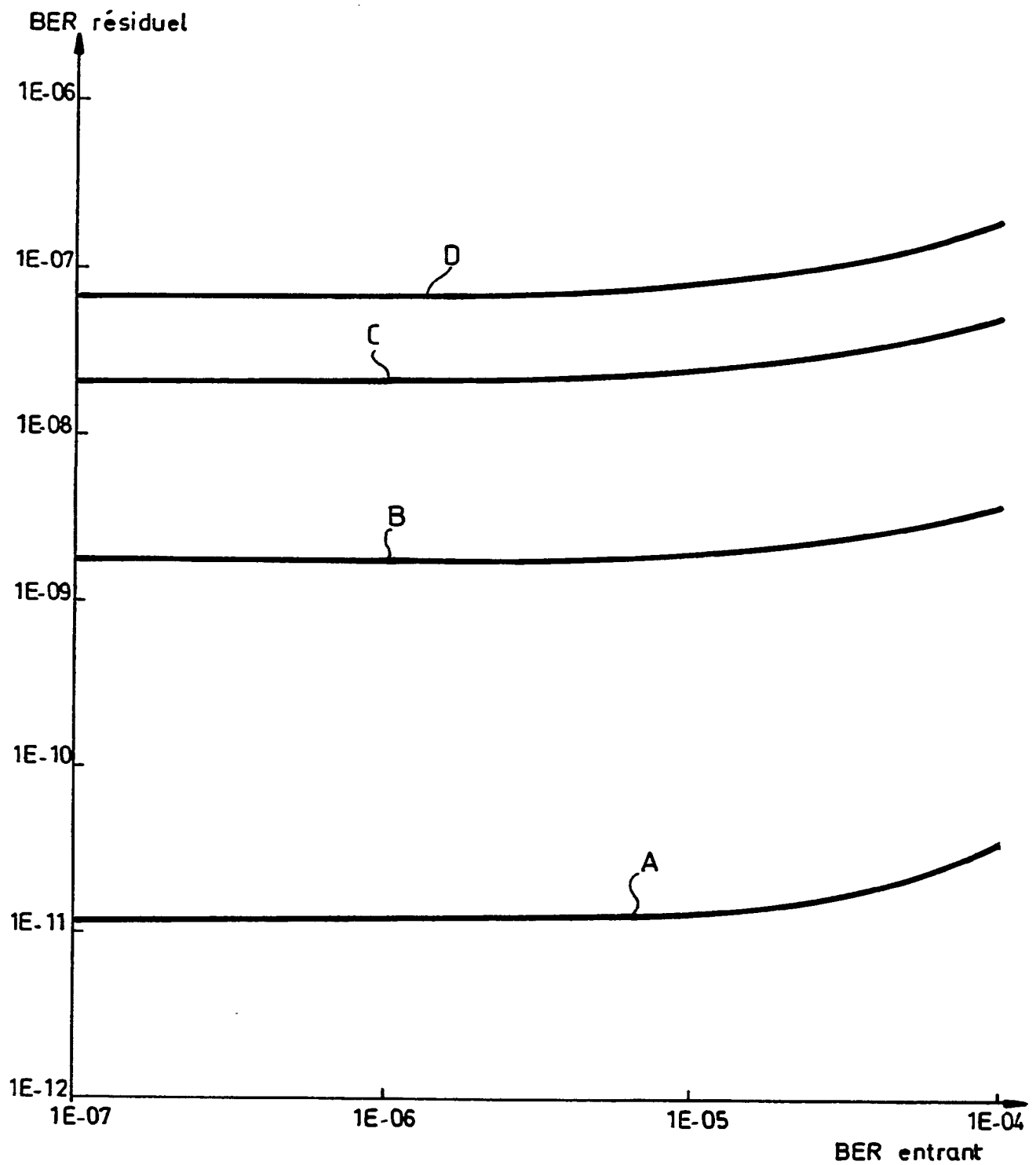


FIG.11

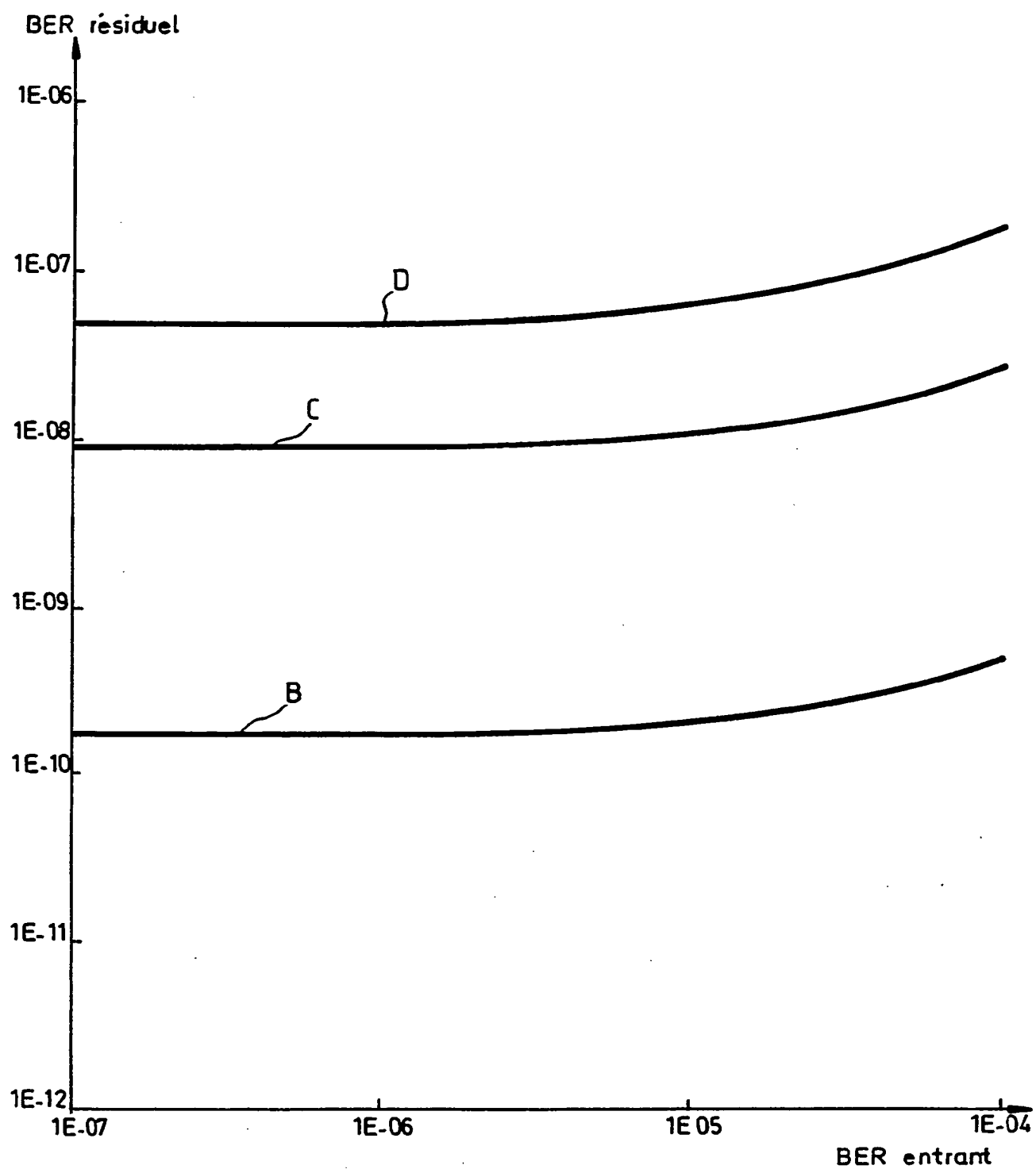


FIG.12

11/11

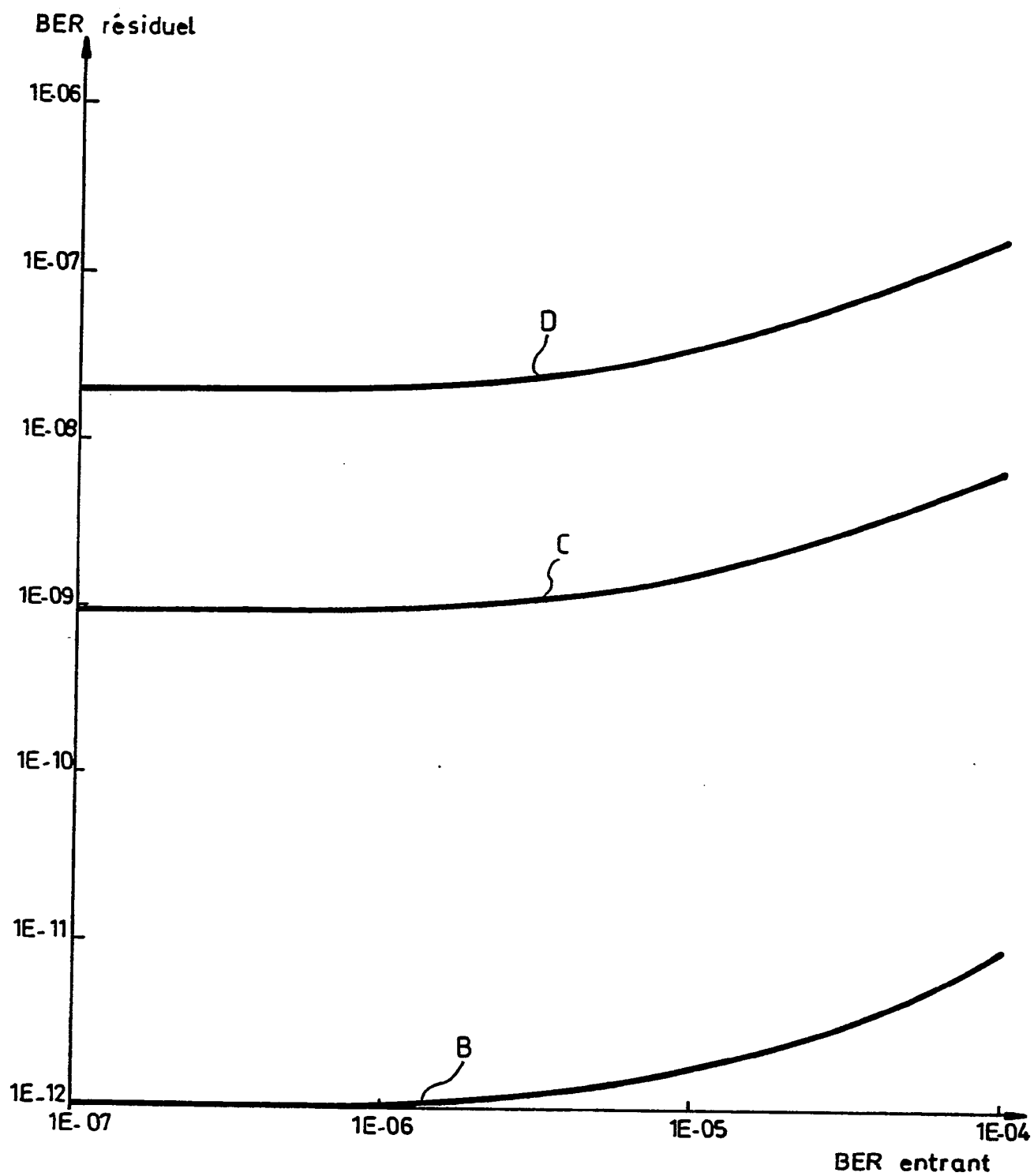


FIG.13